



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

AUG 18 2006

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Guidance on Protecting Personally
Identifiable Information (PII)

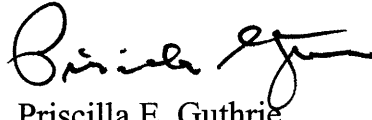
- References: (a) OMB M-06-16, "Protection of Sensitive Agency Information," 23 June
2006
- (b) OMB M-06-19, "Reporting Incidents Involving Personally Identifiable
Information and Incorporating the Cost for Security in Agency
Information Technology Investments," July 12, 2006.
- (c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation,"
February 6, 2003

This memorandum establishes guidance for the protection of Personally Identifiable
Information (PII) in accordance with references (a) and (b).

DoD Components are directed to ensure that all PII not explicitly cleared for public
release is protected according to Confidentiality Level Sensitive, as established in reference (c).
Additionally, all DoD information and data owners shall conduct risk assessments of
compilations of PII and identify those needing more stringent protection for remote access or
mobile computing. The attachment provides detailed implementation guidance.



The points of contact for this memorandum are Donald Jones (703) 614-6640, donald.jones@osd.mil and Gus Guissanie (703) 614-6132, gus.guissanie@osd.mil.

A handwritten signature in black ink, appearing to read "Priscilla Guthrie", with a stylized flourish at the end.

Priscilla E. Guthrie
Principal Deputy
(DoD CIO)

Attachment:

Department of Defense (DoD) Guidance on Protecting Personally Identifiable
Information (PII)

**Department of Defense Guidance on Protecting
Personally Identifiable Information (PII)**

August 18, 2006

Subject: Department of Defense Guidance on Protecting Personally Identifiable Information (PII)

- References: (a) OMB M-06-16, "Protection of Sensitive Agency Information," 23 June 2006
- (b) OMB M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006.
- (c) DoDD 5400.11, "DoD Privacy Program," Nov 16, 2004.
- (d) DoDD 8000.1, "Management of DoD Information Resources and Information Technology," change 1 March 20, 2002
- (e) through (h), see enclosure 1.

1. PURPOSE.

This implements DoD policy regarding the protection of personally identifiable information as established in references (a-c) and according to references (d-h).

2. APPLICABILITY AND SCOPE.

This policy applies to

2.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Component(s)").

2.2. All DoD-owned or controlled information systems or services that receive, process, store, display or transmit DoD information regardless of classification or sensitivity. This includes but is not limited to information systems or services that contain information meeting the criteria for designation as Privacy Act records as defined in reference (c). As established in reference (e) and related issuances, this also includes contracted or outsourced access to DoD information and resources.

3. DEFINITIONS are at enclosure 2.

4. POLICY.

It is DoD policy that:

4.1. All PII shall be evaluated for impact of loss or unauthorized disclosure and protected accordingly.

4.2. All PII electronic records shall be assigned a High or Moderate PII Impact Category according to the definitions established in this policy and protected at a Confidentiality Level of Sensitive or higher as established in reference (e)¹, unless specifically cleared for public release (e.g., the name and contact information for selected public officials). Further, electronic PII records assigned a High Impact Category shall be protected as follows:

4.2.1. Such records shall not be routinely processed or stored on mobile computing devices or removable electronic media without express approval of the Designated Accrediting Authority (DAA) (previously Designated Approving Authority). See reference (f).

4.2.2. Except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores High Impact electronic records shall be restricted to workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive as established in reference (e) (hereinafter referred to as "protected workplaces").

4.2.3. Any mobile computing device containing High Impact electronic records removed from protected workplaces, including those approved for routine processing, shall:

4.2.3.1. Be signed in and out with a supervising official designated in writing by the organization security official.

4.2.3.2. Require certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token to access the device.

¹ Any Mission Assurance Category is acceptable for DoD information systems processing PII.

4.2.3.3. Implement IA Control PESL-1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

4.2.3.4. Encrypt all data at rest, i.e., all hard drives or other storage media within the device as well as all removable media created by or written from the device while outside a protected workplace. Minimally, the cryptography shall be NIST-certified (i.e., FIPS 140-2 or current). See Reference (e), ECCR (Encryption for Confidentiality (Data at Rest)). Information on encryption products and other implementation details can be found at <http://iase.disa.mil>.

4.2.4. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged functions, must conform to both IA Control EBRU-1 (Remote Access for User Functions) and EBRP-1 (Remote Access for Privileged Functions) as established in reference (e).

4.2.5. Remote access to High Impact PII electronic records is discouraged, is permitted only for compelling operational needs, and:

4.2.5.1. Shall employ certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token.

4.2.5.2. The remote device gaining access shall conform to IA Control PESL-1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended). See reference (e).

4.2.5.3. The remote device gaining access shall conform to IA Control ECRC-1, Resource Control. See Reference (e).

4.2.5.4. Download and local/remote storage of PII records is prohibited unless expressly approved by the DAA.

4.2.6. Any High Impact electronic PII records stored on removable electronic media taken outside protected workplaces shall signed in and out with a supervising official and shall be encrypted. Minimally, the cryptography shall be NIST-certified. See Reference (e), ECCR (Encryption for Confidentiality (Data at Rest)).

4.3. Loss or suspected loss of PII shall be reported to:

4.3.1. The United States Computer Emergency Readiness Team (US CERT) within one hour in accordance with the requirements of reference (b) and guidance at www.us-cert.gov, as published.

4.3.2. The DoD Component Privacy Office/Point of Contact (POC) within 24 hours and the DoD Privacy Office within 48 hours or as established by the Defense Senior Privacy Official (paragraph 5.2).

4.4. The underlying incident that led to the loss or suspected loss of PII (e.g., computer incident, theft, loss of material, etc.,) shall continue to be reported in accordance with established procedures (e.g., to designated Computer Network Defense (CND) Service Provider according to reference (g); law enforcement, chain of command, etc.).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer shall address the protection of PII in the management DoD information resources and information technology consistent with reference (d).

5.2. The Director for Administration and Management (DA&M), as the Senior Privacy Official for the Department of Defense shall establish procedures for reporting the loss or suspected loss of PII within the Department of Defense and ensure that incidents involving the loss of PII are addressed consistent with the requirements of reference (c).

5.3. Heads of DoD Components shall:

5.3.1. In accordance with this policy and direction from the DoD Senior Privacy Official, establish reporting procedures to ensure that loss or suspected loss is reported in accordance with paragraphs 4.3 and 4.4 above.

5.3.2 Ensure Information Owners or Data Owners identify PII, evaluate the risk of loss or unauthorized disclosure, assign Impact Categories for electronic PII records, and establish appropriate protection measures for PII in other media.

5.3.3 Ensure Information Assurance Managers in concert with other certification and accreditation team members incorporate protection measures for High Impact electronic PII records into the DoD IA certification and accreditation process as defined in reference (f).

5 3.4. Ensure supervising officials establish logging and tracking procedures for High Impact electronic PII records on mobile computing devices or portable media removed from protected workplaces.

6. PROCEDURES are as specified above and in references (e-h).

7. EFFECTIVE DATE.

This policy is effective immediately.

Enclosures – 3

E1. References, continued

E2. Definitions

E3. Traceability to OMB Checklist

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (f) DoD CIO Memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance," July 6, 2006
- (g) CJCSM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), Change 3, March 8 2006
- (h) DoD CIO Memorandum, "Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance", 28 October 2005

E2. ENCLOSURE 2.

DEFINITIONS

E2.1. Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are “individuals.” Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not “individuals.” Reference (c).

E2.2. Individual Identifier. Information associated with a single individual and used to distinguish him or her from other individuals, e.g., name, social security number or other identifying number, symbol, or other identifying particular such as a finger or voice print or photograph.

E2.3. Personally Identifiable Information (PII). Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. Reference (b).

E2.4. PII Impact Category. For DoD information assurance purposes, consistent with reference (a) and FIPS 199, electronic PII records are categorized according to the potential negative impact of loss or unauthorized disclosure:

E2.4.1. High Impact. Any Defense-wide, organizational (e.g., unit or office), or program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act. Also, any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures. Examples: A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII.

E2.4.2. Moderate Impact. Any electronic records containing PII not identified as High Impact.

E2.5. PII Electronic Record. Any item, collection, or grouping of information in electronic form maintained by a DoD Component that associates personal information such as education, financial transactions, medical history, criminal or employment history, with an individual identifier. Also any item, collection, or grouping of information in electronic form that associates two or more individual identifiers, e.g., name and social security number. Electronic records that contain information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records.

E2.6. Remote Access. Enclave-level access for authorized users external to the enclave that is established through a controlled access point (e.g., a remote access server or communications server) at the enclave boundary. Reference (e) modified to include controlled access point examples.

E1. ENCLOSURE 3.TRACEABILITY TO OMB CHECKLIST

Checklist Item (Reference(a))	DoD Guidance / Methodology	Remarks
Step 1. Confirm the identification of personally identifiable information protection needs.	1. Conduct Privacy Impact Assessments as required by DoD policy, (reference (h)), http://www.dod.mil/nii/pia/	Equivalent to or exceeds PL-5 and associated NIST SP 800-53 controls
	2. Assign DoD Mission Assurance Category (MAC) and Confidentiality Level according to DoDI 8500.2 and review associated IA Controls. Ensure that the minimum Confidentiality Level for any DoD information system processing PII is Sensitive.	Equivalent to or exceeds RA-2 and associated NIST SP 800-53 controls
	3. Identify PII and assign PII Impact Category according to this policy.	Equivalent to or exceeds RA-4 and associated NIST SP 800-53 controls
Step 2. Verify adequacy of organizational policy.		The formulation of this policy was based upon a review of all SP 800-53 controls identified for consideration in the OMB checklist and all DoDI 8500.2 IA Controls, including those mapped in Appendix G to the SP 800-53 controls identified for consideration in the OMB checklist. This policy verifies and updates DoD policy, thus satisfying Step 2 for all DoD information systems and services.

Checklist Item (Reference(a))	DoD Guidance / Methodology	Remarks
<p>Step 3. Implement protections for PII being transported and/or stored offsite.</p> <p>Step 4. Implement protections for remote access to PII.</p>	<p>For Moderate Impact PII, implement the IA Controls assigned according to reference (e). For High Impact PII, incorporate the PII protection measures identified in this policy into assigned IA Controls and C&A activities (e.g., IA Controls Implementation Plan, POAM). Note the PII measures in this policy specifically address PII being transported and/or stored off site and remote access.</p>	<p>Steps 3 and 4 are satisfied as each DoD information system manages compliance with its assigned IA Controls and the measures established in this issuance, if required.</p>